Análisis de la situación actual de la empresa:

La empresa debe proteger información sensible de posibles personas externas no autorizadas y proteger a los clientes para que no les roben la información de cuenta.

El plan de seguridad es:

Utilizar encriptación de datos y ocultar la IP como con VPN. Sugerimos pedir a usuarios que cambien la contraseña periódicamente. Deben delimitar quién puede y debe acceder a la información confidencial e identificar las partes más sensibles y esenciales del sistema.

### Seguridad Fisica

\*\*Dispositivos físicos de protección\*\*

Pararrayos, extintores, detectores de humo, alarma contra intrusos, entre otros.

\*\*UPS (Uninterruptable Power Supply)\*\*

Es un dispositivo electrónico que almacena energía por medio de una batería interna. Esto le permite a los dispositivos que están conectados al mismo, frente a un apagón eléctrico, seguir almacenando la información por un determinado tiempo.

\*\*Respaldo de datos\*\*

Es importante saber que los datos son los activos más importantes dentro de una organización, por tal motivo, es de suma importancia el manejo y cuidado de los mismos ya que pueden estar expuestos a muchos factores como hurto, alteración, virus, entre otros. Por tal motivo, se deben realizar copias de seguridad o backups de los datos completos e incrementales. El backup es un proceso por el cual se realiza la copia de los datos originales con el fin de prevenir cualquier tipo de pérdida de los mismos.

\*\*Sistemas redundantes\*\*

Son la copia de datos de mayor importancia

### \*\*Seguridad Lógica\*\*

La seguridad lógica es un tipo de software que impide que malware o hackers puedan ingresar a nuestra computadora a través de Internet o de una red. Está conformada por un conjunto de procesos que se encargan de garantizar la seguridad de los datos y sistemas, además controlan el acceso a los mismos.

Incluye aspectos como:

- Control de acceso

- Cifrado de datos

- Antivirus

- Firewalls

### \*\*¿Qué es la seguridad activa?\*\*

Los elementos denominados activos contienen información. Estos pueden tener muchas formas: servidores, dispositivos móviles, bases de datos, entre otros. Esos activos contienen información que alguien quiere vulnerar, obtener, destruir, etcétera. Como su intención es acceder a una información, lo va a hacer a través de una vulnerabilidad —problema que tienen los sistemas que contienen información—. \*\*La amenaza aprovecha esa vulnerabilidad para ingresar de forma indebida a la información y hacer lo que quería hacer. La seguridad activa protege y evita daños en los sistemas informáticos.\*\*

Buenas prácticas:

- Uso y empleo adecuado de contraseñas. Una de las técnicas para que una contraseña sea segura consiste en la combinación entre letras, números, mayúsculas y otros caracteres. No se debe usar nombre de mascotas o fechas de nacimiento, entre otros datos que pueden ser de conocimiento público.

- Uso de software de seguridad informática, como antivirus, antiespías y cort

### \*\*¿Qué es la seguridad pasiva?\*\*

Es un conjunto de acciones o técnicas de seguridad que entran en acción para minimizar los daños a los sistemas informáticos. Estas acciones se activan cuando se ha introducido un malware o cualquier otra amenaza en los sistemas.

Buenas prácticas:

- La realización de copias de seguridad de los datos en más de un dispositivo o en distintas ubicaciones físicas.

- Escanear y limpiar continuamente los equipos para controlar y evitar ataques de malware.

- Crear particiones en el disco duro para almacenar archivos y backups (copias de seguridad) en una unidad distinta a donde tenemos nuestro sistema operativo.

- Frente a un ataque, desconectar el equipo de la red hasta que se pueda solucionar.

- Es importante que cuando haya una infección por un virus, se compruebe que el antivirus funcione correctamente.